特 許 協 力 条 約

ＰＣＴ

特許性に関する国際予備報告（特許協力条約第二章）

（法第 12 条、法施行規則第 56 条）
〔ＰＣＴ36 条及びＰＣＴ規則 70〕

出願人又は代理人 の書類記号 CYBER001B	今後の手続きについては、様式ＰＣＴ／ＩＰＥＡ／４１６を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ２００５／００１５２４	国際出願日 （日．月．年）　０２．０２．２００５	優先日 （日．月．年）　０２．０２．２００４
国際特許分類（ＩＰＣ） Int.Cl. *H04L12/66(2006.01)*		
出願人（氏名又は名称） 株式会社サイバー・ソリューションズ		

１．この報告書は、ＰＣＴ35 条に基づきこの国際予備審査機関で作成された国際予備審査報告である。
法施行規則第 57 条（ＰＣＴ36 条）の規定に従い送付する。

２．この国際予備審査報告は、この表紙を含めて全部で　4　ページからなる。

３．この報告には次の附属物件も添付されている。

a．☑ 附属書類は全部で　6　ページである。

☐ 補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関が認めた訂正を含む明細書、請求の範囲及び／又は図面の用紙（ＰＣＴ規則 70.16 及び実施細則第 607 号参照）

☐ 第Ｉ欄４．及び補充欄に示したように、出願時における国際出願の開示の範囲を超えた補正を含むものとこの国際予備審査機関が認定した差替え用紙

b．☐ 電子媒体は全部で＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿（電子媒体の種類、数を示す）。
配列表に関する補充欄に示すように、電子形式による配列表又は配列表に関連するテーブルを含む。
（実施細則第 802 号参照）

４．この国際予備審査報告は、次の内容を含む。

☑ 第Ｉ欄　国際予備審査報告の基礎
☐ 第Ⅱ欄　優先権
☐ 第Ⅲ欄　新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
☑ 第Ⅳ欄　発明の単一性の欠如
☑ 第Ⅴ欄　ＰＣＴ35条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
☐ 第Ⅵ欄　ある種の引用文献
☐ 第Ⅶ欄　国際出願の不備
☐ 第Ⅷ欄　国際出願に対する意見

国際予備審査の請求書を受理した日 １１．１０．２００５	国際予備審査報告を作成した日 １２．０４．２００６
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｘ　９０７７ 吉田　隆之 電話番号　０３－３５８１－１１０１　内線　３５９６

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（２００５年４月）

特許性に関する国際予備報告

国際出願番号　ＰＣＴ／ＪＰ２００５／００１５２４

第Ⅰ欄　報告の基礎

１．言語に関し、この予備審査報告は以下のものを基礎とした。

☑ 出願時の言語による国際出願

☐ 出願時の言語から次の目的のための言語である＿＿＿＿＿＿ 語に翻訳された、この国際出願の翻訳文

☐ 国際調査（ＰＣＴ規則12.3(a)及び23.1(b)）

☐ 国際公開（ＰＣＴ規則12.4(a)）

☐ 国際予備審査（ＰＣＴ規則55.2(a)又は55.3(a)）

２．この報告は下記の出願書類を基礎とした。（法第6条（ＰＣＴ14条）の規定に基づく命令に応答するために提出された差替え用紙は、この報告において「出願時」とし、この報告に添付していない。）

☐ 出願時の国際出願書類

☑ 明細書

第 1,2,6-8,10-13 ページ、出願時に提出されたもの

第 3-5,9 ページ*、2005.10.11 付けで国際予備審査機関が受理したもの

第＿＿＿＿＿＿ ページ*、＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

☑ 請求の範囲

第＿＿＿＿＿＿ 項、出願時に提出されたもの

第＿＿＿＿＿＿ 項*、ＰＣＴ１９条の規定に基づき補正されたもの

第 1-5,7 項*、2005.10.11 付けで国際予備審査機関が受理したもの

第＿＿＿＿＿＿ 項*、＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

☐ 図面

第＿＿＿＿＿＿ ページ／図 、出願時に提出されたもの

第＿＿＿＿＿＿ ページ／図 *、＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

第＿＿＿＿＿＿ ページ／図 *、＿＿＿＿＿＿ 付けで国際予備審査機関が受理したもの

☐ 配列表又は関連するテーブル
配列表に関する補充欄を参照すること。

３．☑ 補正により、下記の書類が削除された。

☐ 明細書　第＿＿＿＿＿＿ ページ

☑ 請求の範囲　第 6,8,9 項

☐ 図面　第＿＿＿＿＿＿ ページ／図

☐ 配列表（具体的に記載すること）＿＿＿＿＿＿

☐ 配列表に関連するテーブル（具体的に記載すること）＿＿＿＿＿＿

４．☐ この報告は、補充欄に示したように、この報告に添付されかつ以下に示した補正が出願時における開示の範囲を超えてされたものと認められるので、その補正がされなかったものとして作成した。（ＰＣＴ規則 70.2(c)）

☐ 明細書　第＿＿＿＿＿＿ ページ

☐ 請求の範囲　第＿＿＿＿＿＿ 項

☐ 図面　第＿＿＿＿＿＿ ページ／図

☐ 配列表（具体的に記載すること）＿＿＿＿＿＿

☐ 配列表に関連するテーブル（具体的に記載すること）＿＿＿＿＿＿

＊ ４．に該当する場合、その用紙に〝superseded〟と記入されることがある。

第Ⅳ欄　発明の単一性の欠如

１．☑ 請求の範囲の減縮又は追加手数料の納付命令書に対して、出願人は、規定期間内に、

☐ 請求の範囲を減縮した。

☑ 追加手数料を納付した。

☐ 追加手数料及び、該当する場合には、異議申立手数料の納付と共に、異議を申し立てた。

☐ 追加手数料の納付と共に異議を申し立てたが、規定の異議申立手数料を支払わなかった。

☐ 請求の範囲の減縮も、追加手数料の納付もしなかった。

２．☐ 国際予備審査機関は、次の理由により発明の単一性の要件を満たしていないと判断したが、ＰＣＴ規則68.1の規定に従い、請求の範囲の減縮及び追加手数料の納付を出願人に求めないこととした。

３．　国際予備審査機関は、ＰＣＴ規則 13.1、13.2 及び 13.3 に規定する発明の単一性を次のように判断する。

☐ 満足する。

☑ 以下の理由により満足しない。

補正後の請求項１には、不正攻撃が行われていると判断する条件として４つの条件が記載されており、これら４つの条件のうちの１つの条件を用いて不正攻撃が行われていると判断するから、実質的に４つの発明が記載されていると認められる。
そして請求項１の４つの発明と請求項４が単一の一般的発明概念を形成するように連関する一群の発明であるとは認められない。

請求項１の(a)はフィールド値の数の時間的な変化の比率を判断すること
請求項１の(b)(c)は、フィールド値の数とパケット数の比率を用いて判断すること
請求項１の(d)はフィールド値の数と通信量の比率を用いて判断すること
請求項４は２つ以上のフィールド値の組み合わせの数を用いて判断すること

であって、不正と判断する条件は全体として４つの群である。

フィールド値を用いて不正攻撃が行われていると判断することは、先の国際調査報告で記載したように先行技術であるから、PCT 規則 13.2 の第２文の意味において、特別な技術的特徴ではない。

４．　したがって、国際出願の次の部分について、この報告を作成した。

☑ すべての部分

☐ 請求の範囲 ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿ に関する部分

第Ⅴ欄　新規性、進歩性又は産業上の利用可能性についての法第12条（ＰＣＴ35条(2)）に定める見解、それを裏付ける文献及び説明

１．　見解

新規性（Ｎ）	請求の範囲	１－５，７	有
	請求の範囲		無
進歩性（ＩＳ）	請求の範囲	１－５，７	有
	請求の範囲		無
産業上の利用可能性（ＩＡ）	請求の範囲	１－５，７	有
	請求の範囲		無

２．　文献及び説明（ＰＣＴ規則70.7）

文献１：JP 2003-283571 A(日本電信電話株式会社)2003.10.03
文献２：JP 2004-140524 A(ソニー株式会社)2004.05.13
文献３：WO 01/88731 A1(NIKSUN INC.)2001.11.22

請求の範囲１
文献１には、【0043】～【0049】を参照すれば、送信元アドレスのばらつき度合いが高い場合に攻撃を検出できること、TTL値を用いた検査がDDoS攻撃の検査方法として可能であることが記載されており、複数の通信装置に分散させることにより、攻撃元を探索することも記載されている。
文献２の第２実施例、【0044】～【0057】には、所定処理時間に間に受信したパケットの総数がｐを超えた場合、送信元アドレス数が所定値以上の場合にDoS攻撃であると判定する検知システムが記載されている。
文献３には、クレーム９－１６を参照すれば、無効アドレスの数の閾値の超過に対応して警報信号を発生するデータ処理方法が記載されている。

しかし、(a)フィールド値の数の時間的な変化、(b)(c)フィールド値の数とパケット数の比率、(d)フィールド値の数と通信量の比率により攻撃を検出すること、はいずれの文献にも記載されていない。

文献１の【0044】、【0045】にはばらつき度合いにより攻撃を検出することが記載されているが、文献１のばらつき度合いは送信元アドレス毎の出現回数の分布に大小が存在するか、一様に多いかを判断しており、パケット数に対する送信元アドレス数の比率により判断しているものではない。

請求の範囲４
フィールド値の組み合わせの数をカウントして攻撃を検出することはいずれの文献にも記載されていない。

請求の範囲２，３，５，７
請求の範囲１または４を引用しており、上記と同様の理由により進歩性を有する。

ることを目的とする。

課題を解決するための手段

[0015] 請求項１に係る発明は、インターネット回線を通じて送信されてきたパケットのヘッダ内のあるフィールドの値の数を監視し、該フィールドの値の数が一定時間内で所定率に達した場合には不正攻撃が行われていると判定することを特徴とする不正情報検知システムである。

フィールドの値としては、例えば、次のものが上げられる。

バージョン
ヘッダ長
ToS
全長
アイデンティフィケーション
フラグ
フラグメントオフセット
Time to Live
プロトコル
ヘッダチェックサム
発信元アドレス
到達先アドレス
オプション
ポート

あるフィールドの値の数は、例えばフィールドの値が「発信元アドレス」の場合、区別できる発信元アドレスとして、a1(＝一郎)、a2(＝二郎)、a3(＝三郎)、・・・・an(＝ｎ郎)があった場合、フィールドの値の数はｎである。

[0016] 前記所定率は下記のいずれかの条件により算出される。

(a) 時刻ｔから一定時間内におけるフィールドの値の数 N(t)が、任意の時点 t_1 から一定時間内におけるフィールドの値の数 $N(t_1)$ と比較して k_1 倍（k_1：予め定めた閾値）以上になった場合、すなわち比率が $N(t)/N(t_1) \geqq k_1$ となった場合に不正攻撃と判定する。

(b) 時刻ｔから一定時間内におけるフィールドの値の数 N(t)とパケット数 P(t)との比率 N(t)/P(t)を求めて、該比率が予め定めた閾値 k_2 以上になった場合、すなわち $N(t)/P(t) \geqq k_2$ となった場合に不正攻撃と判定する。

(c) 上記(b)で求めた時刻ｔにおける比率 N(t)/P(t)が、任意の時点 t_1 の比率 $N(t_1)/P(t_1)$ と比較して k_3 倍（k_3：予め定めた閾値）以上になった場合、すなわち

$\{N(t)/P(t)\} / \{N(t_1)/P(t_1)\} \geqq k_3$ となった場合に不正攻撃と判定する。

(d) 時刻 t から一定時間内におけるフィールドの値の数 N(t)と通信量（オクテット数／ビット数）T(t)との比率 N(t)/T(t)を求めて、該比率が予め定めた閾値 k_4 以上になった場合、すなわち $N(t)/T(t) \geqq k_4$ となった場合に不正攻撃と判定する。

[0017] 請求項２に係る発明は、前記フィールドの値は、個々のフィールドの値の２つ以上の任意の組合せをフィールドの値として構成することを特徴とする請求項１に記載の不正情報検知システムである。

[0018] 例えば、フィールドの値として「発信元アドレス」と「到達先アドレス」との組合せによりフィールドの値を構成する。

[0019] まず前記同様、発信元アドレスとして、a1(＝一郎)、a2(＝二郎)、a3(＝三郎)、・・・・an(＝ｎ郎)があったとする。

[0020] ak（ｋ＝１～ｎ）について、到達アドレスの種類が mk 個あるとすると、この場合における複数のフィールドの組合せにより構成されるフィールドの値の数は Σmk（ｋ＝１～ｎ）となる。

[0021] 請求項３に係る発明は、インターネット回線を通じて送信されてきたパケットのヘッダ内にある TTL(Time To Live)値に基づいたホップ数が、予め定めた所定の値の範囲から外れた場合には不正攻撃が行われていると判定することを特徴とする請求項１に記載の不正情報検知システムである。

[0022] 前記パケットのヘッダ内にある送信元アドレスが詐称されたものではなく正規のものである場合、ホップ数はほぼ決まった値となることから、所定の値の範囲を予め設定しておくことで、ホップ数が前記所定の値の範囲から外れた場合に不正攻撃が行われていると判定することが可能になる。

[0023] 請求項４に係る発明は、インターネット回線を通じて送信されてきたパケットのヘッダ内のあるフィールドの値の数を監視し、個々のフィールドの値の２つ以上の任意の組合せをフィールドの値として構成し、該フィールドの値の数が一定時間内で所定数に達した場合には不正攻撃が行われていると判定する手段を備えたことを特徴とする不正情報検知システムである。

[0024] 請求項５に係る発明は、インターネット回線を通じて送信されてきたパケットのヘッダ内にある TTL 値に基づいたホップ数が、予め定めた所定の値の範囲から外れた場合には不正攻撃が行われていると判定することを特徴とする請求項４に記載の不正情報検知システムである。

[0025] 前記パケットのヘッダ内にある送信元アドレスが詐称されたものではなく正規のものである場合、ホップ数はほぼ決まった値となることから、所定の値

の範囲を予め設定しておくことで、ホップ数が前記所定の値の範囲から外れた場合に不正攻撃が行われていると判定することができる。

[0026] 請求項６に係る発明は、請求項１乃至５に記載の不正情報検知システムを、インターネットの複数個所に設置することで不正攻撃の送信元を探索するようにしたことを特徴とする不正攻撃元探索システムである。

[0027] インターネットの複数個所に不正情報検知システムを設置して、各箇所で不正攻撃が行われているか判定する。例えば、２つの観測点で不正攻撃を検知した場合、２つの観測点を結ぶ経路を不正攻撃が通過したと判定することができるため、複数の観測点で不正攻撃が行われているか判定することで、不正攻撃の通過した経路を追跡することができ、不正攻撃の送信元を探索することができる。

発明の効果

[0028] 本発明の不正情報検知システムによれば、同時に大量に送信されてきたパケットに対し、該パケットのヘッダ内のあるフィールド値の数が一定時間内に所定率に達した時に、略同期して送信元アドレス件数が所定率に達した場合には、その大量のパケットを(D)DoS 攻撃パケットと判定することにより、特定の送信元アドレスに対して受信許可設定若しくは受信拒否設定をするといった細かく煩わしい設定をすることなく(D)DoS 攻撃が送信されてきたことを認識および追跡することができる。

図面の簡単な説明

[0029] [図１]本発明の(D)DoS 攻撃検知およびその追跡システムの概念図である。

[図２]（Ａ）はパケットデータフォーマットの説明図、（Ｂ）は通信量の一例を時系列で示したグラフ図、（Ｃ）はパケットのアドレス件数の一例を時系列で示したグラフ図である。

[図３]パケット探索を示す概念図である。

[図４]インターネットのシステムを示す概念図である。

符号の説明

[0030] １…インターネット回線

２…送信側コンピュータ

３…受信側コンピュータ

４…通信監視装置（判定手段）

カテゴリは一つ、ないしは複数のヘッダ領域によって定められるパケットを分類できる性質のことである。

(カテゴリの例) プロトコル領域がTCPであるパケット全て便宜上"Total カテゴリ"というカテゴリを定義する。全てのパケットはこのカテゴリに属する。

[0048] 今までの統計分析手法は、モニタや探査装置により観測されたパケットから全ての観測パケット数や、あるカテゴリに対するパケット観測数などの標本値を元にしてきた。

[0049] [表1]

(例) プロトコル領域毎のパケット数

	全体	TCPパケット	UDPパケット	ICMPパケット
10:01	181	123	46	0
10:02	142	100	32	10
10:03	206	140	0	13
10:04	217	120	87	10

カテゴリ変換 (C-Transform) における統計分析では、検知したパケットが属するカテゴリの数に着目する。上記の例において、プロトコル領域ごとのカテゴリの数を見た場合以下の通りになる。

[表2]

	全体	TCPパケット	UDPパケット	ICMPパケット	カテゴリの数
10:01	181	123	46	0	2
10:02	142	100	32	10	3
10:03	206	140	0	13	2
10:04	217	120	87	10	3

このようにパケットの数の分布からカテゴリの数の分布を作成する方法のことをカテゴリ変換"C-Transform" と呼ぶ。

[0050] いくつかのヘッダ領域の和によって作成されたカテゴリがとる事が可能な最大のカテゴリの数はその領域の合わせた幅による。例えば幅が合わせて4ビットの領域で作成されるカテゴリの場合、最大のカテゴリの数は16個 (2の4乗) である。

[0051] しかし、IPヘッダにおけるVersion領域とProtocol領域のように、予め定義された以外の値を持つことができないヘッダ領域がある(ASSIGNED NUMBERS, RFC 790 参照)

請求の範囲

[1] （補正後）インターネット回線を通じて送信されてきたパケットのヘッダ内のあるフィールドの値の数を監視し、該フィールドの値の数が一定時間内で所定率に達した場合には不正攻撃が行われていると判定する手段を備えること、および前記所定率は下記のいずれかの条件により算出されることを特徴とする不正情報検知システム。

(a) 時刻tから一定時間内におけるフィールドの値の数N(t)が、任意の時点t_1から一定時間内におけるフィールドの値の数$N(t_1)$と比較してk_1倍（k_1：予め定めた閾値）以上になった場合、すなわち比率が$N(t)/N(t_1) \geqq k_1$となった場合に不正攻撃と判定する。

(b) 時刻tから一定時間内におけるフィールドの値の数N(t)とパケット数P(t)との比率N(t)/P(t)を求めて、該比率が予め定めた閾値k_2以上になった場合、すなわち$N(t)/P(t) \geqq k_2$となった場合に不正攻撃と判定する。

(c) 上記(b)で求めた時刻tにおける比率N(t)/P(t)が、任意の時点t_1の比率$N(t_1)/P(t_1)$と比較してk_3倍（k_3：予め定めた閾値）以上になった場合、すなわち$\{N(t)/P(t)\} / \{N(t_1)/P(t_1)\} \geqq k_3$となった場合に不正攻撃と判定する。

(d) 時刻tから一定時間内におけるフィールドの値の数N(t)と通信量（オクテット数／ビット数）T(t)との比率N(t)/T(t)を求めて、該比率が予め定めた閾値k_4以上になった場合、すなわち$N(t)/T(t) \geqq k_4$となった場合に不正攻撃と判定する。

[2] （補正後）前記フィールドの値は、個々のフィールドの値の２つ以上の任意の組合せをフィールドの値として構成することを特徴とする請求項１に記載の不正情報検知システム。

[3] （補正後）インターネット回線を通じて送信されてきたパケットのヘッダ内にあるTTL値に基づいたホップ数が、予め定めた所定の値の範囲から外れた場合には不正攻撃が行われていると判定することを特徴とする請求項１に記載の不正情報検知システム。

[4] （補正後）インターネット回線を通じて送信されてきたパケットのヘッダ内のあるフィールドの値の数を監視し、個々のフィールドの値の２つ以上の任意の組合せをフィールドの値として構成し、該フィールドの値の数が一定時間内で所定数に達した場合には不正攻撃が行われていると判定する手段を備えたことを特徴とする不正情報検知システム。

[5] （補正後）インターネット回線を通じて送信されてきたパケットのヘッダ内にあるTTL値に基づいたホップ数が、予め定めた所定の値の範囲から外れた場合には不正攻撃が行われていると判定することを特徴とする請求項４に記載の不正情報検知システム。

[6] （削除）

[7] （補正後）請求項１乃至５に記載の不正情報検知システムを、インターネットの複数個所に設置することで不正攻撃の送信元を探索するようにしたことを特徴とする不正攻撃元探索システム。

[8] （削除）

[9] （削除）